Ringe

Sisam Khanal

June 5, 2024

Definition 1. Ring $(R, +, \cdot)$ mit inneren Verknüpffung $+ : R \times R \to R$ (der Addition) und $\cdot : R \times R \to R$ (der Multiplikaion heißt **Ring**, wenn gilt:

- $(R, +)$ ist eine ablesche Gruppe,
- $(R, \cdot)$ ist eine Halbgruppe (ohne Identität)
- $a(b + c) = ab + ac$ und $(a + b)c = ac + bc$ für alle $a, b, c \in R$ (Distributivgesetze).

Definition 2. Einheitengruppe Sei R ein Ring mit 1. Ein Element $a \in R$ heißt *invertierbar* oder eine *Einheit*, wenn es ein $b \in R$ gibt mit $ba = 1 = ab$. Die Einheiten bilden eine Gruppe

$$R^\times = \{a \in R |\ a \text{ ist invertierbar } \}$$

Beachte, dass $R^\times$ kein Teilring ist.

Beispiel

- $\mathbb{Z}^\times = \{\pm 1\}$
- $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

Definition 3. Nullteiler Ein Element $a \neq 0$ eines Ringes R heißt **Nullteiler** von R genannt, wenn ein $b \neq 0$ in R existiert mit $ab = 0$ oder $ba = 0$.

Definition 4. Integritätsringe Ein kommutativer, nullteilerfreier Ring mit 1 heißt **Integritätsringe** oder **Integritätsbereich**.

Hiervon folgt für $ab = 0 \implies a = 0$ oder $b = 0$ und für $ac = bc \implies a = b$

Beispiel

- $\mathbb{Z}$ ist ein Integritätsring
- Der Teilring $\mathbb{Z}[i] := \{a + ib \mid a, b \in \mathbb{Z}\}$ der *ganze Gauß'schen Zahlen* ist Integritätsbereich.
- Der Restklassenring $\mathbb{Z}/p\mathbb{Z}$ ist genau dann ein Integritätsring, wenn p prim ist.
- $R[X]$ ist ein Integritätsring. Es gilt weiterhin $R[X]^\times = R^\times$

Definition 5. Ideale Eine Untergruppe A von $(R, +)$ heißt **Ideal** von R, wenn gilt:

- $a \in A, r \in R \implies ra \in A \ : RA \subseteq A$
- $a \in A, r \in R \implies ar \in A \ : AR \subseteq A$

Gilt nur $RA \subseteq A$ bzw. $AR \subseteq A$ für eine Untergruppe A von $(R, +)$, so nennt man **Links-** bzw. **Rechtsideal**. Wenn ein Ring Links- und Rechtsideal ist, dann ist der Ring **Ideal** von R. Alle Ideale sind Teilring

Beispiel

- $\{0\}$ und R sind die trivialen Ideale des Ringes R.
- Die Ideale von $\mathbb{Z}$ sind genau die Mengen $n\mathbb{Z}$ mit $n \in \mathbb{N}_0$
- Sei $1 \in A$ ein Ideal, dann $A = R$
- $\left\{ \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$ ist ein *Linksideal* aber kein *Rechtsideal*
- $\left\{ \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$ ist *Rechtsideal* aber kein *Linksideal*

Theorem 1. *Für jede Familie $(A_i)_{i \in I}$ von Idealen A_i von R ist auch $A := \bigcap_{i \in I} A_i$ ein Ideal von R .*

Beispiel

$(2\mathbb{Z}) \cap (3\mathbb{Z}) \cap (4\mathbb{Z}) = 12\mathbb{Z}$